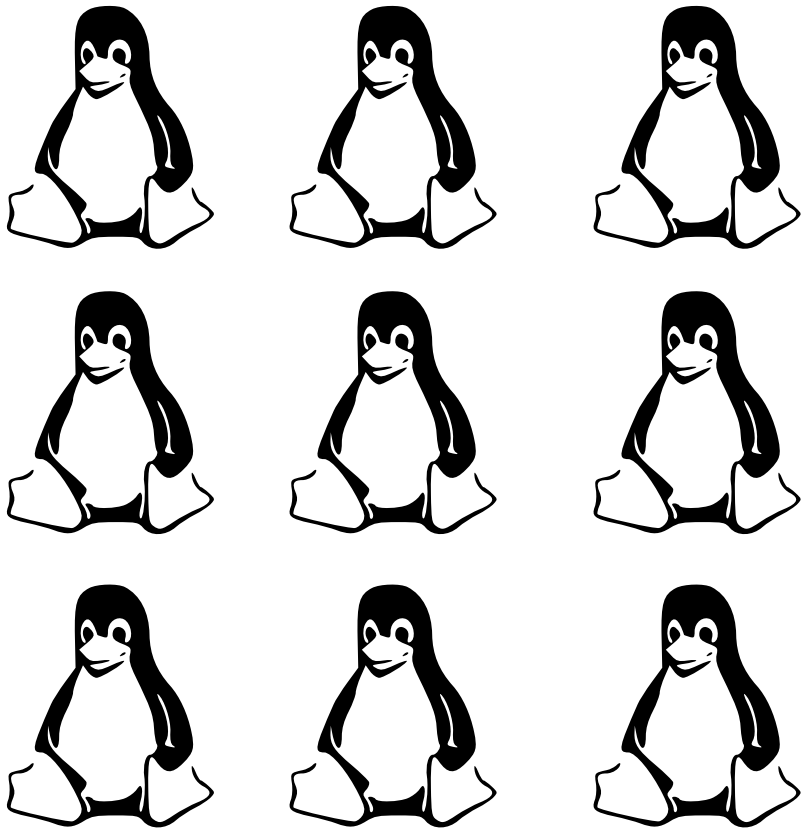
Linux 101

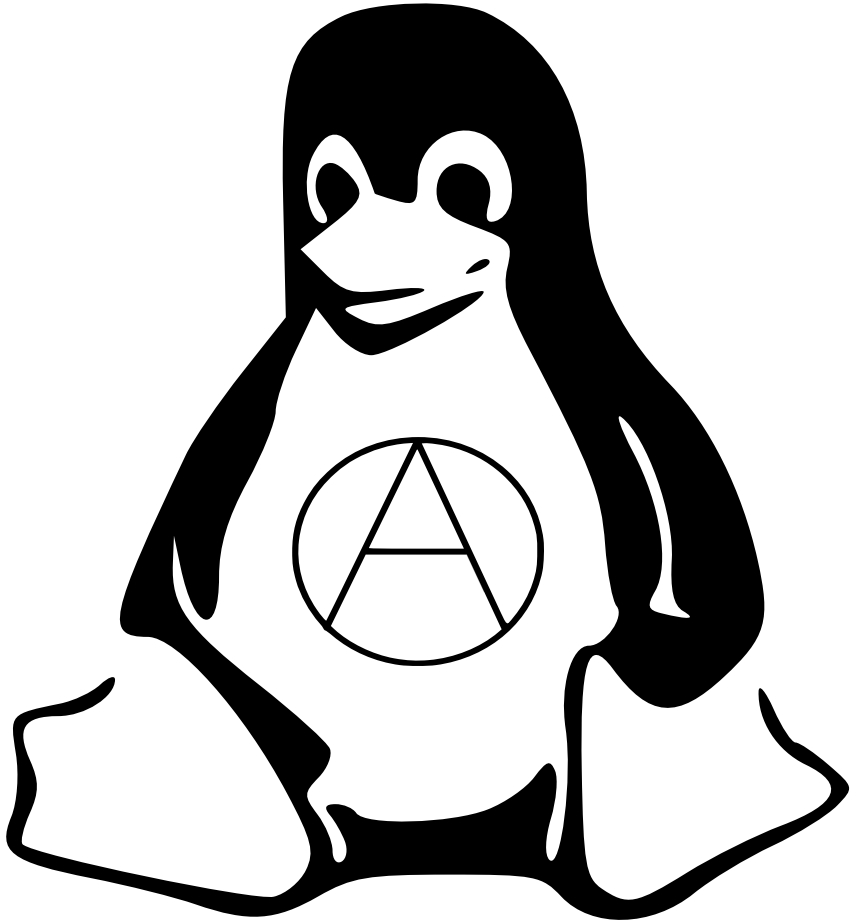


ftp://distro

Written & formatted by FTP DISTRO

Blog:
https://ftpdistro.noblogs.org
Twitter:
https://twitter.com/ftpdistro
Instagram:
https://instagram.com/ftp.distro
Store:
https://ftpdistro.github.io

https://tails.boum.org/



~$sudo make totaldestroy

Table Of Contents

1. Introduction [Page 3]
2. Installation [Page 5]
3. File structure [Page 23]
4. Command line tips & tricks [Page 28]
5. Downloading packages [Page 36]
6. KALI tools [Page 37]
7. TAILS tools [Page 45]

1. Introduction

So you want to start using Linux as an operating system instead of (or perhaps in addition to) Windows or Mac OSX. You might be asking yourself: "Where to begin? Which flavor of Linux should I use? How do I install software? How do I use a terminal?". This 'zine will explore all of these questions. Here is a quick rundown on the history of the operating system itself (from wikipedia):

"The Linux kernel is a free and open-source, monolithic, modular, multitasking, Unix-like operating system kernel. It was conceived and created in 1991 by Linus Torvalds for his i386-based PC, and it was soon adopted as the kernel for the GNU operating system, which was created as a free replacement for UNIX. Since then, it has spawned a plethora of operating system distributions, commonly also called Linux.

Linux is deployed on a wide variety of computing systems, such as embedded devices, mobile devices (including its use in the Android operating system), personal computers, servers, mainframes, and supercomputers. It can be tailored for specific architectures and for several usage scenarios using a family of simple commands (that is, without the need of manually

Sound Juicer to rip audio CDs

BookletImposer to convert linear PDF documents into booklets, and vice-versa

Encryption and privacy

Support for both **LUKS** and **VeraCrypt** encrypted volumes (like USB sticks)

GnuPG, the GNU implementation of **OpenPGP** for email and data encyption and signing

GNOME screen keyboard for accessibility, and as a countermeasure against hardware keyloggers

MAT to anonymize metadata in files

KeePassXC password manager

GtkHash to calculate checksums

PDF Redact Tools to redact and strip metadata from text documents before publishing

Tesseract OCR to convert images containing text into a text document

FFmpeg to record and convert audio and video

Download at:

HTTPS Everywhere transparently enables SSL-encrypted connections to a great number of major websites
NoScript to have even more control over JavaScript.
uBlock Origin to remove advertisements.

Pidgin preconfigured with OTR for Off-the-Record Messaging

OnionShare for anonymous file sharing

Thunderbird email client with support for **OpenPGP** and **RSS** and **Atom** news feeds

Aircrack-ng for wireless network auditing

Electrum, an easy-to-use bitcoin client

Desktop edition

LibreOffice

Gimp and **Inkscape** to edit images

GNOME Sound Recorder for recording sound

Audacity for recording and editing sounds

Simple Scan and **SANE** for scanner support

Brasero to burn CD/DVDs

editing its source code before compilation); privileged users can also fine-tune kernel parameters at runtime. Most of the Linux kernel code is written using the GNU extensions of GCC to the standard C programming language and with the use of architecture specific instructions (ISA). This produces a highly optimized executable (vmlinux) with respect to utilization of memory space and task execution times.

Day-to-day development discussions take place on the Linux kernel mailing list (LKML). Changes are tracked using the version control system git, which was created by Torvalds as a bespoke replacement for BitKeeper. Linux as a whole is released under the GNU General Public License version 2 (GPLv2), but it also contains several files under other compatible licenses, and an ad hoc exemption for the user space API header files (UAPI)."

It is important to remember that Linux gives you full control over your system, and we mean that in every sense. This means that if you mess something up with root permissions it can alter the entire operating system. Luckily there is a large community online that runs into some of the issues you might encounter. StackOverflow is a great resource for this! It is important (as is always) to create backups of your files --- both offline and online (cloud storage). If you

are someone with radical politics, Linux is great for privacy conscious users because the code is open-source. This means that any security researcher can audit the code for software vulnerabilities.

2. Installation

Linux (usually) allows the ability to try out specific distributions before making a final install. The three main distributions that you will find online are Debian, Ubuntu and Arch. All of them come with different quirks and abilities, with each flavor having varied levels of support for the project. Many beginner Linux users stick with Ubuntu at first. Within each distribution is a Desktop Environment, or DE for short. Try each one out when booting up LiveCD/USBs! You can find a compilation of different OS "images" on the website https://distrowatch.com/. You can flash these OS images to a flash drive, SD card or a DVD. To create a live Linux stick, you will need to grab the ISO image of your preferred distribution. This can be done by going to the download page and downloading the ISO image onto your computer. Once this step is done, you will need to ‘write’ the contents of the ISO file to your USB stick. Moreover, The USB device must be formatted properly.

is a privacy-focused operating system that can run on a liveCD/USB without installing the OS on your device's hard drive. All inbound and outbound connections are forced through the TOR protocol. TOR, or The Onion Router, is used to hide IP location metadata when browsing the web. This can be useful for journalists or whistleblowers. The OS will leave no digital footprint on the machine by default unless explicitly told to do so.

Included software

GNOME, an intuitive and attractive desktop environment

Networking

Tor with:
stream isolation, regular, obfs3, and obfs4 bridges support

The Onion Circuits graphical frontend

NetworkManager for easy network configuration

Tor Browser, a web browser based on **Mozilla Firefox** and modified to protect your anonymity with:
all cookies are treated as session cookies by default;

that makes it one of the best Kali Linux tools available. It checks in against potentially dangerous files/programs, outdated versions of server, and many more things.

20. Yersinia

Yersinia is an interesting framework to perform Layer 2 attacks (Layer 2 refers to the data link layer of OSI model) on a network. Of course, if you want a network to be secure, you will have to consider all the seven layers. However, this tool focuses on Layer 2 and a variety of network protocols that include STP, CDP, DTP, and so on.

21. Social Engineering Toolkit (SET)

If you are into pretty serious penetration testing stuff, this should be one of the best tools you should check out. Social engineering is a big deal and with SET tool, you can help protect against such attacks.

Download at:
https://www.kali.org/get-kali/

7. TAILS OS

TAILS (The Amnesic Incognito Live System)

Once you figure out a particular distribution that you want to install permanently you can go thru the process while booting up the liveCD/USB. Some guides will explain how to do this from an existing Linux distribution install on the users computer, but we can assume that you haven't gotten that far yet. This part of the guide will focus on installion on both Windows and Mac OSX.

Create a Linux Live USB Drive from Mac OS

You can create a bootable Linux drive from Mac OS. However, you will need to perform some extra operations to ensure the live USB is fully compatible with your Apple hardware. First of all, you will need the USB device and the ISO image of your preferred Linux distribution.

How to Create a Linux Bootable USB Using the GUI on Mac

Users of Apple’s Mac OS can easily create Linux installation media using Etcher. It is a simple and powerful GUI tool that makes creating bootable USB devices easier for beginners.

Step - 1: Prepare the USB Device

To prepare the USB stick for a live Linux USB, first, reformat the device using Apple's 'Disk Utility' application. You can open 'Disk Utility' by going to the 'Applications>Utilities' menu or using Spotlight search. Once the application is opened, insert your USB device and inspect whether it has been added to Disk Utility. Make sure to enable the option 'View>Show All Devices'.

Now, select your USB stick and click on the 'Erase' option from the toolbar to start reformatting your device. Set the format option of the USB drive to MS-DOS (FAT) and the scheme option to GUID Partition Map. Check if everything is selected appropriately, and then click on 'Erase'.

Step - 2: Install and Open Etcher

We will make use of free and open-source software called Etcher (https://www.balena.io/etcher/) for creating our bootable USB drive. You can download Etcher for Mac from its download page. Once the package has been downloaded and mounted, you can run it in-place or drag it to the Applications folder. Since recent versions of Mac OS blocks applications from unidentified developers, you may need to click on the 'Open Anyway' option to run Etcher.

logging capability? Snort has got your back. Even being an open source intrusion prevention system, it has a lot to offer.

The official website mentions the procedure to get it installed if you don't have it already.

17. Autopsy Forensic Browser

Autopsy is a digital forensic tool to investigate what happened on your computer. Well, you can also use it to recover images from SD card. It is also being used by law enforcement officials. You can read the documentation to explore what you can do with it.

You should also check out their GitHub page.

18. King Phisher

Phishing attacks are very common nowadays. And, King Phisher tool helps test, and promote user awareness by simulating real-world phishing attacks. For obvious reasons, you will need permission to simulate it on a server content of an organization.

19. Nikto

Nikto is a powerful web server scanner -

13. Apktool

Apktool is indeed one of the popular tools found on Kali Linux for reverse engineering Android apps. Of course, you should make good use of it - for educational purposes.

With this tool, you can experiment some stuff yourself and let the original developer know about your idea as well. What do you think you'll be using it for?

14. sqlmap

If you were looking for an open source penetration testing tool - sqlmap is one of the best. It automates the process of exploiting SQL injection flaws and helps you take over database servers.

15. John the Ripper

John the Ripper is a popular password cracker tool available on Kali Linux. It's free and open source as well. But, if you are not interested in the community-enhanced version, you can choose the pro version for commercial use.

16. Snort

Want real-time traffic analysis and packet

Step - 3: Configure Etcher for ISO Installation

The Etcher workflow consists of three stages. First, you need to select the ISO file. Simply click on the 'Select image' option, and Etcher will provide a file explorer that can be used to locate and select the ISO image. Once this is done, click on 'Select drive' and select your USB device. Etcher will select the USB device automatically if one is already connected.

Once the above two stages are completed, you can click on the 'Flash' option. This will start the writing process and will ask you for your user password.

Step - 4: Wait Till Etcher Finishes

After you have entered your password, the flash process will begin. Etcher will display the writing progress, speed, and the estimated duration to complete. Once the ISO has been flashed, Etcher will perform a validation operation to check whether the data contained in the USB device is the same as the ISO. Your Linux bootable USB drive is ready to boot after this step completes successfully.

Step - 5: Booting into Live Linux on Mac

To boot into a Linux installation media from Mac, you will need to restart your device and press the Option/alt key. Make sure the USB device is inserted while doing this. It will launch the ‘Startup Manager’ and display a list of bootable devices connected to your Apple machine. The live USB should be labeled as ‘EFI Boot’ and usually appears in a gold or yellow color. Select this device, and it will start booting into the Linux distribution.

How to Create a Linux Bootable USB Using the Terminal on Mac

If you are an advanced user, you might want to create your live USB from the terminal. Follow the below steps to create your live installation media using the Mac terminal successfully.

Step – 1: Convert the ISO File to IMG File

To create a live USB from the terminal, you will need to convert the ISO image of your chosen Linux distro to an IMG file. This can be done by using the hdiutil tool. Simply fire up a terminal session and issue the following command.

$ hdiutil convert /path/to/ubuntu.iso

However, this is not a free tool anymore, you can try it free for 7 days on from its official website.

11. Burp Suite Scanner

Burp Suite Scanner is a fantastic web security analysis tool. Unlike other web application security scanner, Burp offers a GUI and quite a few advanced tools.

However, the community edition restricts the features to only some essential manual tools. For professionals, you will have to consider upgrading. Similar to the previous tool, this isn’t open source either.

I’ve used the free version, but if you want more details on it, you should check out the features available on their official website.

12. BeEF

BeEF (Browser Exploitation Framework) is yet another impressive tool. It has been tailored for penetration testers to assess the security of a web browser.

This is one of the best Kali Linux tools because a lot of users do want to know and fix the client-side problems when talking about web security.

assessments, the report generated by Skipfish will come in handy.

9. Maltego

Maltego is an impressive data mining tool to analyze information online and connect the dots (if any). As per the information, it creates a directed graph to help analyze the link between those pieces of data.

Do note, that this isn't an open source tool.

It comes pre-installed, however, you will have to sign up in order to select which edition you want to use. If you want for personal use, the community edition will suffice (you just need to register for an account) but if you want to utilize for commercial purpose, you need the subscription to the classic or XL version.

10. Nessus

If you have a computer connected to a network, Nessus can help find vulnerabilities that a potential attacker may take advantage of. Of course, if you are an administrator for multiple computers connected to a network, you can make use of it and secure those computers.

-format UDRW -o /path/to/target.img

OS X often appends the .dmg extension after the output image. However, you do not need to worry about that since it will not affect the installation.

Step -2: Determine the USB Device

You need to determine the device node assigned to your USB stick before you can write the target image to it. You can do it by running the following command.

$ diskutil list

This will show a list of currently connected devices. Now, plug in your USB device and rerun the command. Compare the output of the two commands to determine the device node.

Step - 3: Unmount the USB Device

Before you start to write the IMG file, make sure to unmount the USB drive. You can easily do this by issuing the following command.

$ diskutil unmountDisk /dev/diskX

You need to replace X with the disk number of your device. You should have this information from completing step number

two.

Step – 4: Write the IMG File to USB

Now that we have converted the ISO file and unmounted the USB device, we can create the Linux bootable USB. Enter the following command in your terminal session to start the writing process.

$ sudo dd if=/path/to/target.img of=/dev/diskX bs=1m

Make sure to replace the input file's location with the actual location of the target.img file. Also, replace /dev/diskX with the actual disk number of your device. Moreover, if you see the error "dd: Invalid number '1m'", then you are using the GNU dd instead of BSD dd. Simply replace 1m with 1M to mitigate this issue.
Pro Tip: Using /dev/rdiskX in place of /dev/diskX will make the writing process much faster!

Step – 5: Eject and Remove USB Device

Once the write operation finishes, eject the USB device by running the following command.

$ diskutil eject /dev/diskN

Remove the USB when this process is

as well.

It is being actively maintained, so I would definitely recommend trying this out. And it's really easy to install Wireshark on Linux.

7. Metasploit Framework

Metsploit Framework is the most used penetration testing framework. It offers two editions – one (open source) and the second is the pro version to it. With this tool, you can verify vulnerabilities, test known exploits, and perform a complete security assessment.

Of course, the free version won't have all the features, so if you are into serious stuff, you should compare the editions here.

8. Skipfish

Similar to WPScan, but not just focused for WordPress. Skipfish is a web application scanner that would give you insights for almost every type of web applications. It's fast and easy to use. In addition, its recursive crawl method makes it even better.

For professional web application security

vulnerabilities.

4. Aircrack-ng

Aircrack-ng is a collection of tools to assess WiFi network security. It isn't just limited to monitor and get insights - but it also includes the ability to compromise a network (WEP, WPA 1, and WPA 2).

If you forgot the password of your own WiFi network - you can try using this to regain access. It also includes a variety of wireless attacks with which you can target/monitor a WiFi network to enhance its security.

5. Hydra

If you are looking for an interesting tool to crack login/password pairs, Hydra will be one of the best Kali Linux tools that comes pre-installed.

It may not be actively maintained anymore - but it is now on GitHub, so you can contribute working on it as well.

6. Wireshark

Wireshark is the most popular network analyzer that comes baked in with Kali Linux. It can be categorized as one of the best Kali Linux tools for network sniffing

finished. Now you can restart your Mac and boot into the Linx live distro. Press the Option/alt key while the USB is inserted for launching the 'Startup Manager'. The live USB should be labeled as 'EFI Boot'. Select this device, and it will start booting into the Linux distribution.

Create a Linux Live USB Drive from Windows

You can create a live Linux installation media on Windows using a GUI toolkit like Rufus or via the command prompt. The following sections discuss both of these. We are assuming you are on Windows 10. However, these methods should also work the same for Windows 8.

How to Create a Linux Bootable USB Using the GUI on Windows

We will use Rufus for creating a live Linux USB from Windows. You can download Rufus from its website. Install it once the download finishes and follow the below steps.

Step - 1: Select USB Device

To select the USB device, launch Rufus, and insert your USB. Rufus should detect the

device automatically. In case there are multiple USB devices connected to your machine, select the appropriate one from the Device field. We recommend users to unplug all other USB devices to make this step hassle-free.

Step – 2: Select Boot Options and Partition Scheme

Once you have selected the right USB device, go to the ‘Boot selection’ menu. Here you will find two options – ‘FreeDOS’ and ‘Non Bootable’. Select FreeDOS and move on to the next options. Both the ‘Partition scheme’ and ‘Target system’ options should be selected automatically by Windows.

Step – 3: Select the ISO File

Given you have already downloaded the ISO file of your preferred Linux distro, select it by clicking the ‘SELECT‘ button. It will open the file explorer that can be used to browse the file system and locate the ISO. Mark the appropriate ISO image and click ‘Open‘ to select the ISO.

Step – 4: Write the ISO File

Once you have selected the ISO file, the Volume Label will be updated accordingly. Leave all other fields as they are and

It also offers features for firewall evasion and spoofing.

2. Lynis

Lynis is a powerful tool for security auditing, compliance testing, and system hardening. Of course, you can also utilize this for vulnerability detection and penetration testing as well.

It will scan the system according to the components it detects. For example, if it detects Apache – it will run Apache-related tests for pin point information.

3. WPScan

WordPress is one of the best open source CMS and this would be the best free WordPress security auditing tool. It’s free but not open source.

If you want to know whether a WordPress blog is vulnerable in some way, WPScan is your friend.

In addition, it also gives you details of the plugins active. Of course, a well-secured blog may not give you a lot of details, but it is still the best tool for WordPress security scans to find potential

using the sudo pacman -S examplepackage command. To remove the package, use the -R option (sudo pacman -R examplepackage).

In Fedora Linux the command dnf install examplepackage will carry out this task.

6. KALI Linux Tools

If you decide to try and learn pentesting (penetration testing or security testing), Kali Linux comes preloaded with 100s of command line & GUI tools that you can try out. You will need to look up how to setup a proper simulated environment using VMs (virtual machines) in order to legally pentest and practice improving your skills. Youtube is a great resource for learning how to setup secure VMs in VirtualBox for pentesting. Here is a quick rundown of (some of) the tools that come pre-loaded with Kali Linux as of 2021:

1. Nmap

Nmap or “Network Mapper” is one of the most popular tools on Kali Linux for information gathering. In other words, to get insights about the host, its IP address, OS detection, and similar network security details (like the number of open ports and what they are).

click on START to begin the writing process.

Step – 5: Approve Additional Downloads and Warning

Rufus may need to download some modules to complete the writing process. Approve any such requests by clicking on the Yes button. Rufus will show another prompt with some warnings related to ISOHybrid images.

Keep the recommended options (Write in ISO Image mode) and click Ok. The next screen will ask for confirmation regarding the USB write process. Enter OK to continue the installation.

If you get any more warnings, approve them as well. If everything goes alright, Rufus will start copying the contents of the ISO image to the USB device. You can view the progress in the lower right corner of the window.

It can take up to 15 minutes to complete the process. Once Rufus finishes, the progress bar will turn green and display the text ‘READY‘. Your live USB is now ready to boot.

How to Create a Linux Bootable USB Using the

Windows CMD Prompt

You can also create the live Linux media using the CMD prompt of your Windows machine. Follow the below steps to do this. Make sure you have already downloaded the ISO file of your chosen Linux distribution.

Step - 1: Insert USB Device

Insert the USB device to your machine and select do nothing if a prompt appears. The device should have at least 4 GB of free space available to it. Try plugging the USB device into a high-speed port for faster writing.

Step - 2: Run DISKPART

DISKPART is a command-based Windows tool for disk partitioning. Open your CMD prompt as administrator and run the following command to invoke DISKPART.

```
C:\Windows\system32> diskpart
```

Step - 3: List Available Disks

Once DISKPART is open, use the below command to display all the available disk drives.

```
DISKPART> list disk
```


take a very diverse set of parameters from users and, based on those changes, the file permission.

chown The chown command is very much similar to the chmod command. But instead of changing access permissions, it enables users to change the ownership of a file or directory. Both the chmod and chown terminal commands require root privileges to run.

5. Downloading packages

Downloading packages and software in Linux can be a varied process. In some cases, it is as cut and dry as typing a few commands (sudo apt install examplepackage && sudo apt update in both Debian and Ubuntu) or downloading a Applimage from a software repository and running chmod -x on the Appimage. In some other cases, it can be somewhat frustrating and becomes a rabbit hole of downloading new dependencies over and over again. On some Github/Gitlab repositories you will find easy instructions for installation. In other instances, you might need to resort to search or post on StackOverflow.

In Arch Linux downloading a package is done

Linux Commands That Deal With I/O And Ownership

clear The clear command is handy to clear out your existing terminal screen. Often you will find the need to wipe out the terminal screen after some earlier Linux commands leave your terminal screen with a garbled output.

echo The echo command is a very powerful command-line utility that lets you output a specific text to the terminal console. Type in echo followed by some texts within parentheses to find out for yourself. What's more interesting for this command is that you can pipe the output to other terminal commands.

sort The sort command is quite compelling at the things it does. Whenever you find the need to sort out a file in an alphabetical or reverse manner, utilize this command.

sudo The sudo command is the holy grail of Linux commands. It lets non-privileged users access and modify files that require low-level permissions. Often you will use this command to access root from your regular user account.

chmod The chmod command is among the most powerful Linux commands you will use to change or modify the access permissions of system files or objects. This command can

This will show a list of disks. You can determine your USB stick by looking at the column that's labeled size.

Step - 4: Select USB Device

Now, you need to select your USB device so you can format it. Enter the following command in your DISKPART prompt.

DISKPART> select disk X

Replace X with the disk number of your USB device. Once you do this, DISKPART will select your USB device for further configuration.

Step - 5: Create Primary Partition

Before creating the primary partition for your USB, clean the device by issuing the following command.

DISKPART> clean

Once DISKPART completes the cleaning process, issue the following command to create the primary partition.

DISKPART> create partition primary

Step - 6: Select and Activate the Partition

After you have created the primary partition, you need to select and activate it. You can do this by running the following commands in your CMD prompt.

DISKPART> select parition X

Replace X with the appropriate partition number and proceed to the next command.

DISKPART> active

This will make the selected partition active.

Step – 7: Format the Partition

Now you need to format the selected partition. You can do this by running the following command in your DISKPART prompt.

DISKPART> format fs=ntfs quick

This can take somewhere between 10 to 15 minutes, depending on the write speed of your USB device and port. Once this step is finished, you need to add a drive letter to it.

Step – 8: Assign Drive Letter

DISKPART> assign

used Linux commands to search for files from the terminal. This compelling yet flexible terminal command allows users to search for files based on certain criteria such as file permissions, ownership, modification date, size, etc.

which The which command is pretty useful if all you are trying to search are executable files. This handy little terminal command takes specific parameters and searches for binary files in the $PATH system environment variable based on them very effectively.

locate The locate command is one of those Linux commands that are used for finding the location of a specific file. It is one of the most straightforward terminal commands that you can leverage when not sure about the location of a particular file on your Linux machine.

grep grep command is among the most powerful regular expression terminal commands you can use when searching for patterns inside large volumes of text files. It will take the pattern you're looking for as input and search the specified files for that particular pattern.

sed This is one of the most widely used Linux commands to manipulate each line of a file or stream by replacing specified parts. It is used heavily by users that deal with large volumes of text data and need to change them on the go.

commands that can be used in scripts or cronjobs and provides users the ability to use the HTTP, HTTPS, and FTP internet protocol.

iptables The iptables command invokes a terminal utility that lets system admins control the incoming and outgoing internet traffic on a particular host machine. It is among the most used Linux commands sysadmins use on a regular basis to define authentic traffics and for blacklisting suspicious or untrusted network requests.

traceroute This command is widely used by security professionals who leverage this command with other terminal commands for determining the route a network packet takes on its way from one machine to another. This is a compelling network command by using which you can safeguard your computer from a number of harmful intruders.

curl cURL is a very powerful network tool that makes transferring files over a network a child's play for even new Linux system users. This is one of those Linux commands designed to work without user interaction and is typically employed in network-related shell scripts.

Linux Commands for Search and Regular Expression

find The find command is one of the most

DISKPART will now assign a drive letter to your USB device. We will assume it's U:\ for the rest for this guide. Yours will differ, so take note of it carefully. Once this is done, you can quit DISKPART by issuing the following command.

DISKPART> exit

Step - 9: Mount the ISO Image

To copy the contents of the ISO image to your newly partitioned USB device, you will need to mount it to the file system. Run the following command in your CMD prompt to start mounting the ISO.

C:\Windows\system32> PowerShell Mount-DiskImage

After a few seconds, PowerShell Mount-DiskImage will ask for the path to the ISO file. Supply the appropriate path in the input field to mount the ISO image.

ImagePath[0]: c:\isoimages\linux\ubuntu.iso

This will mount the ISO file to your Windows file system. Make sure to use a path that reflects the location of your ISO file. It will be assigned a new drive letter. We will assume it is V:\ for the rest of this

tutorial.

Step – 10: Copy the contents of the ISO

Now that's everything is configured, we are ready to copy the contents of the ISO image to the USB device. Use the following command to do this from your CMD prompt.

C:\Windows\system32> XCOPY V:*.* /s /e /f U:

Make sure you are using the right drive letters before you run this command. Replace U:\ with the drive letter assigned to your USB drive and V:\ with the letter assigned to your ISO drive. Once copying is finished, you can quit the CMD prompt and use the live Linux USB for booting into your new Linux distro.

Boot Your Linux Installation Media

If you're booting the Linux system on the same computer you created installation media on, you don't even need to unplug your USB drive. You'll just have to reboot your PC and boot it from the Linux installation media.

To do so, select the "Restart" option in Windows. Your PC may automatically boot from the inserted USB drive and into Linux.

put file upload 'file' from local to remote computer
get file Download 'file' from remote to local computer
quit Logout

Process commands

bg	To send a process to the background
fg	To run a stopped process in the foreground
top	Details on all Active Processes
ps	Give the status of processes running for a user
ps PID	Gives the status of a particular process
pidof	Gives the Process ID (PID) of a process
kill PID	Kills a process
nice	Starts a process with a given priority
renice	Changes priority of an already running process
df	Gives free hard disk space on your system
free	Gives free RAM on your system

Sysadmin commands

wget This is one of the best Linux commands network admins leverage to download files from the web right from the terminal. This is among those handy little terminal

$VARIABLE	
env	Displays all environment variables
VARIABLE_NAME=variable_value	Create a new variable
Unset	Remove a variable
export Variable=value	To set value of an environment variable

User management commands of linux

sudo adduser username	Add a user 'username'
sudo passwd -l 'username'	Set password for 'username'
sudo userdel -r 'username'	Delete User 'username'
finger	Gives information on all logged in users
finger username	Gives information of a particular user

Networking commands

SSH username@ip-address or **hostname** login into a remote Linux machine using SSH
Ping hostname="" or **=""** To ping and Analyzing network and host connections
dir Display files in the current directory of a remote computer
cd "dirname" change directory to “dirname” on a remote computer

If your computer just boots back into Windows, you may have to press a certain key to access a boot device menu and select it during the installation process. Common keys you may have to press during the boot process include F12, Escape, F2, and F10. You may see this key displayed on screen during the boot process.

You may also have to access your BIOS or UEFI firmware settings screen and change the boot order. The exact process will depend on your model of PC. Check your PC’s instructions for more information. (If you built your own PC, check the motherboard’s instruction manual.)

Try Linux

With Linux booted, you’ll get a “live” Linux desktop you can use just as if Linux was installed on your PC. It isn’t actually installed yet and hasn’t modified your PC in any way. It’s running entirely off the USB drive you created (or the disc you burned.)

For example, on Ubuntu, click “Try Ubuntu” instead of “Install Ubuntu” to try it out.

You can explore the Linux system and use it. Bear in mind that it will likely

perform more quickly once it's installed to your PC's internal storage. If you just want to play with Linux for a bit and don't want to install it yet, that's fine—just reboot your PC and remove the USB drive to boot back into Windows/OSX.

If you'd like to try out multiple Linux distributions, you can repeat this process and try a bunch of them before choosing to install one.

(Not all Linux distributions offer a live environment you can play with before you install them, but the vast majority do.)

Warning: Back Up Before Continuing

Before you actually go through with installing Linux, we recommend backing up your important files. You should always have recent backups, especially when you're messing with your system like this.

It should be possible to install Linux in a dual-boot scenario and have the Linux installer seamlessly resize your Windows partition without affecting your files. However, mistakes can happen when resizing partitions. And it would be possible to accidentally click the wrong option and wipe your Windows partition.

mkdir directoryname	Creates a new directory in the present working directory or a at the specified path
rmdir	Deletes a directory
mv	Renames a directory
pr -x	Divides the file into x columns
pr -h	Assigns a header to the file
pr -n	Denotes the file with line numbers
lp -nc , lpr c	Prints "c" copies of the file
lp-d lp-P	Specifies name of the printer

File Permission commands

ls-l	to show file type and access permission
r	read permission
w	write permission
x	execute permission
-=	no permission
Chown user	For changing the ownership of a file/directory
Chown user:group filename	change the user as well as group for a file or directory

Environment Variables commands

echo	To display value of a variable

ls	Lists all files and directories in the present working directory
ls-R	Lists files in sub-directories as well
ls-a	Lists hidden files as well
ls-al	Lists files and directories with detailed information like permissions, size, owner, etc.
cd or **cd ~**	Navigate to HOME directory
cd ..	Move one level up
cd	To change to a particular directory
cd /	Move to the root directory
cat > filename	Creates a new file
cat filename	Displays the file content
cat file1	Joins two files
file2 > file3	(file1,file2) and stores the output in a new file (file3)
mv file "new file path"	Moves the files to the new location
mv filename new_file_name	Renames the file to a new filename
sudo	Allows regular users to run programs with the security privileges of the superuser or root
rm filename	Deletes a file
man	Gives help information on a command
history	Gives a list of all past commands typed in the current terminal session
clear	Clears the terminal

So, before continuing, we encourage you to back up all your important data—just in case.

Install Linux

If you're happy with your Linux distribution and it works well on your PC, you can choose to install it. The Linux distribution will be installed on an internal system drive, just like Windows/OSX.

There are two ways to do this: You could install Linux in a "dual-boot" configuration, where it sits alongside your Windows/OSX operating system on your hard drive and lets you choose which operating system you want to run each time. Or, you can install Linux over Windows/OSX, removing the Windows/OSX operating system and replacing it with Linux. If you have two hard drives, you can even install Linux on one of the hard drives and use them in a dual-boot scenario.

We recommend installing Linux in a dual-boot configuration to give yourself the option of which to use. If you know you really don't want to use Windows/OSX and you want to reclaim some hard disk space, however, go ahead and remove Windows/OSX. Just bear in mind that you'll lose all your installed

applications and any files you haven't backed up.

To perform the installation process, run the installer from the live Linux system. It should be easy to find—it's generally an icon placed on the default live desktop.

The installation wizard will guide you through the process. Go through the installer and choose the options you want to use. Read the options carefully to ensure you're installing Linux in the way you want to. In particular, you should careful not to erase your Windows/OSX system (unless you want to) or install Linux onto the wrong drive.

When the installation process is done, you'll be asked to reboot your PC. Reboot and remove the USB drive or DVD you installed Linux from. Your computer will boot Linux instead of Windows/OSX—or, if you chose to install Linux in a dual-boot scenario, you'll see a menu that will let you choose between Linux and Windows/OSX every time you boot.

3. File structure

Something to remember is that in Linux, everything is a file. Or, more accurately,

send and receive information from various processes running in the Linux environment.

/root - This is the equivalent to the /home folder specifically for the root user, also called the superuser. You really don't want to touch anything in here unless you know what you're doing.

/sbin - Similar to /bin, except that it's dedicated to certain commands that can only be run by the root user, or the superuser.

/tmp - This is where temporary files are stored, and they are usually deleted upon shutdown, which saves you from having to manually delete them like is required in Windows.

/usr - Contains files and utilities that are shared between users.

/var - This is where variable data is kept, usually system logs but can also include other types of data as well.

4. Command line tips & tricks

Basic Linux commands

somewhat equivalent to the Program Files folder on Windows, although it's not exactly the same. Unlike Windows, libraries can be shared between many different programs, which results in Linux installations typically being much more lightweight than Windows, because typically in Windows each program needs it's own library installed, even if it's redundant and already exists for another program. Surely a benefit of Linux file system structure.

/media - Another place where external devices such as optical drives and USB drives can be mounted. This varies between different Linux distros.

/mnt - This is basically a placeholder folder used for mounting other folders or drives. Typically this is used for Network locations, but you could really use it for anything you want. I used to use it as the mount point for my media server's hard drive (/mnt/server).

/opt - Optional software for your system that is not already managed by your distro's package manager.

/proc - The "processes" folder where a lot of system information is represented as files (remember, everything is a file). It basically provides a way for the Linux kernel (the core of the operating system) to

everything is represented as being a file, while in Windows it may be displayed as being a disk drive.

For example, in Windows the hard drive is typically represented as C:\ in the file explorer, and it will even display a little icon of the hard drive and display how much space is being used. In Linux, on the other hand, the hard drive as represented merely as /dev/sda, which is really just a folder/directory, which in Linux is really just a file that points to other files.

So let's take some other more practical examples. The Linux equivalent of your Documents folder in Windows would be /home/username/Documents, whereas in Windows it's typically C:\Users\UserName\Documents. These are actually pretty similar, but you can see where the differences lie.

So using the above Linux file system chart, we need to explore what each folder in the Linux file system is for, which will help us to better understand how Linux works in general. Note that not every folder listed here or pictured above necessarily appears in every Linux distro, but most of them do.

/ - this is known as "root", the logical beginning of the Linux file system structure. Every single file path in Linux begins from root in one way or another. /

contains the entirety of your operating system.

/bin - Pronounced “bin” (as opposed to “bine”), this is where most of your binary files are stored, typically for the Linux terminal commands and core utilities, such as cd (change directory), pwd (print working directory), mv (move), and so on.

/boot - This is where all the needed files for Linux to boot are kept. Many people, including myself, like to keep this folder in it’s own separate partition on the hard drive, especially when dual-booting is involved. A key thing to note is that even when /boot is stored on different partition, it is still logically located at /boot as far as Linux is concerned.

/dev - This is where your physical devices are mounted, such as your hard drives, USB drives, optical drives, and so on. We’ve already explored that typically, your system hard drive is mounted under /dev/sda, whereas your USB thumb drive might be mounted under /dev/sde. You may also have different partitions on your disk, so you’ll see /dev/sda1, /dev/sda2, and so on. In Windows, when you go to “My Computer” or “Computer” and you can see all of the physical devices and drives connected to your computer, this is the equivalent of /dev in Linux file structure.

/etc - Pronounced “et-see”, although some also prefer to spell it out, is where configuration files are stored. Configurations stored in /etc will typically affect all users on the system; whereas users can also store configuration files under their own /home folders, which will only affect that particular user.

/home - This is where you’ll spend the overwhelming majority of your time, as this is where all of your personal files are kept. The Desktop, Documents, Downloads, Photos, and Videos folders are all stored under the /home/username directory. You can also store files directly in your /home folder without going to a sub-folder, if you wish so. Typically, when you open a command-line terminal in Linux, the default location that the terminal points to is your /home/username folder, unless you’ve manually changed the default location to something else.

/lib - This is where libraries are kept. You’ll notice that many times when installing Linux software packages, additional libraries are also automatically downloaded, and they almost always start with lib-something. These are basically the files needed for your programs on Linux to work. You can think of this folder as